V5 Security Guide for Clients

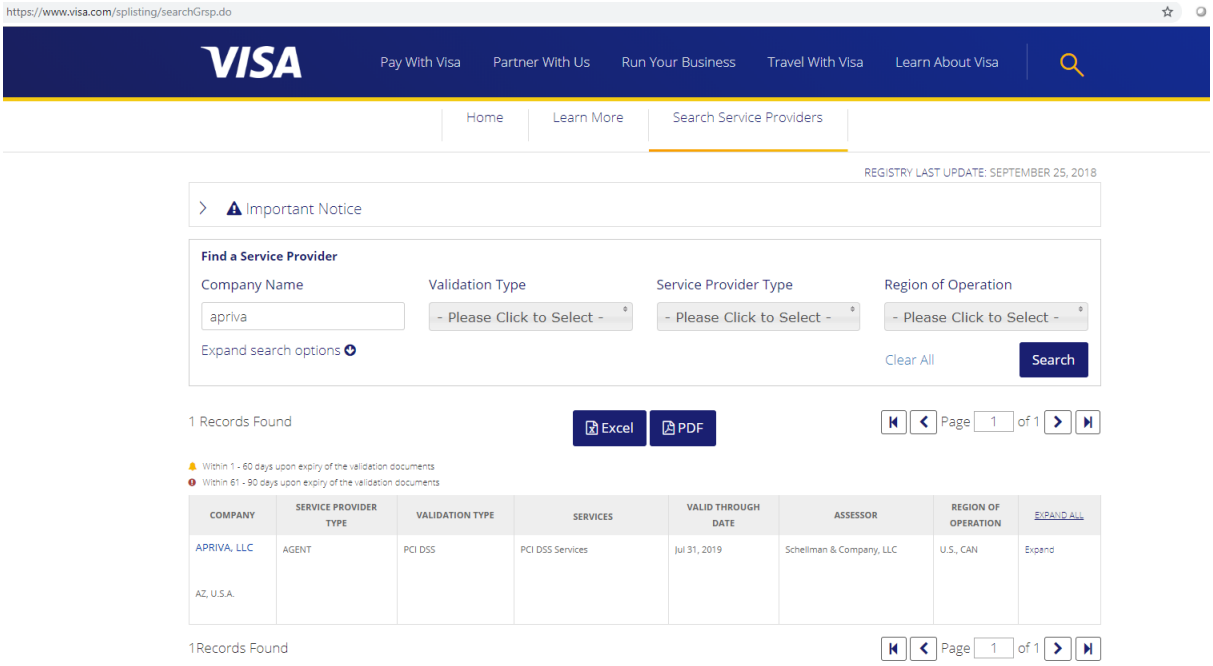
This document explains the basic security PCI DSS compliance information for 365 Retail Markets Kiosk. Please contact Robert Hering at **888-365-6282 ext. 160** or **Robert.Hering@365smartshop.com** with any questions related to this document.

Security of Device

V5 Kiosks utilize a secure direct real-time connection to the card processor when items are checked out. The transactions are card present, with no cardholder data stored for later use. Transactions are needed to complete purchase of items from the self-service, stand-alone, kiosks and mini-retail shops where 365 Retail Markets provide their services. All data is encrypted by the card reader at time of card swipe, 365 Retail Markets does not have access to the encryption keys and cannot decrypt this encrypted cardholder data. This dramatically reduces the scope as 365 Retail Markets does not store, processes and/or transmit (PAN data encrypted during transmission, but 365 Retail Markets does not have access to keys – hence not in scope)

Credit Card Data

365 Retail Markets is PCI DSS Certified. Apriva's Integration Services are PCI DSS Certified and support advanced security features, like card encryption at swipe, card tokenization, and EMV technology. http://www.apriva.com/pos/products/apriva-integration-services



http://www.visa.com/splisting/searchGrsp.do

Card Holder Data Processing

Apriva operates as a payment gateway service. Apriva provides wireless (cellular), wired (PSTN) and internet payment transaction services for merchant clients. Merchant clients

connect to Apriva's application server tier by the aforementioned communications channels, and application servers interact with database servers that contain stored cardholder data. These systems then communicate transactions to other processing entities, which return authorization messages that Apriva provides to the merchant customer. Apriva stores the PAN encrypted in a SQL database.

Remote Access

- TeamViewer is used for Remote Viewing
- Putty (SSH) is used for Command Line Scripts
- DashWeb is used for Software Updates, Real Time analytics, Notifications
- Meraki Z1 is used for VPN connection which provides an encrypted connection

Patching

- Our kiosks our mirrored from Production Yum Server hosted at AWS

Data Storage and Encryption

- AWS (Amazon Web Services) is where all data from the kiosks is stored
- RDS Encryption is used for all data in transit and at rest
- Additional Certificates for AWS can be found here: https://aws.amazon.com/certification/

Privacy, Biometrics and Terms & Conditions Policies

- Our policies can be enabled on our kiosks for GDPR and BIPA consent from account users before creating an account and using biometrics.
- Also, these policies can be located at https://365retailmarkets.com/consumer-policy

Networks

Wireless Networks

Third party wireless or Wi-Fi (802.11x) wireless devices are not supported and cannot be connected to the Card Data Environment.

Corporate Versus Dedicated Networks

The 365 V5 Kiosk requires network connectivity for credit card processing and receiving updates. Operators have two primary options for establishing network connectivity at most client locations, corporate and dedicated networks.

V5 Security Guide for Clients

Many corporate environments (offices, hospitals, etc.) contain existing networks to provided Internet connectivity throughout a building. These corporate networks often restrict the types of information that can be transmitted on them. Corporate networks are typically managed by a dedicated team member(s) who can advise on the feasibility of allowing your kiosk to operate on their existing Internet connection.

A dedicated network, (which for the purposes of this document) constitutes a completely separate network that operators would install, circumvents many challenges that a corporate network may present. A dedicated network could consist of a DSL line, 3G/4G Wireless card, or other dedicated high-speed connection. As the kiosk owner, the operator would need to organize this new, dedicated service to be installed into the client's environment.

Corporate Network*	**Dedicated Network****
Pros	**Pros**
Internet service already in place. No additional cost to the operator.	No need to ask client IT staff to open access or run wiring to a new location
Network is typically very fast compared to DSL or cellular Internet service	The operator owns the network, and therefore requires less coordination to ensure PCI best practices are being followed
Typically managed by dedicated personnel at the client location with knowledge of troubleshooting and secure networking protocols	If cellular is chosen, you have the added mobility to move the kiosk and internet together as needed
Cons	**Cons**
The operator may need to coordinate and implement the correct and secure settings with the client IT staff/network administrator	The operator needs to organize, implement and pay for Internet service
Wiring is typically run to a single location, making kiosk mobility challenging.	Network connectivity (especially cellular) may be slower than a corporate network
The operator is responsible for ensuring the corporate network follows PCI standards which often requires more coordination with client IT staff	When service is interrupted (power surge, modem needs reset) the operator is responsible to respond to troubleshoot the outage.
	May require an operator resource with IT and networking knowledge to ensure the best practices are outlined in this guide. (365 Retail staff is available to assist with secure network setup)

*If the operator chooses to use a corporate network it is the operator's responsibility to ensure this guide is followed by the client network administrator. Be sure to supply them a copy of this guide early in the implementation process paying special attention to the Networks section.

V5 Security Guide for Clients

**If the operator chooses to use a dedicated network, it is your responsibility to ensure the best practices outlined in this guide are followed.

Network Segmentation for Corporate Networks

For deploying on a corporate network, segmenting the kiosk into a secure card data business environment is required. Network segmentation is a strategy intended to simplify PCI DSS compliance of your network and to help you protect your business from hackers. At the most basic level, there are three zones representing three levels of risk.

- **Untrusted Environment –** Network connections that anonymous people have access to be considered "untrusted." They should have no network access to your business computers and POS equipment. Business computers should never be connected directly to this zone. Common untrusted networks are the internet connection itself, customer wireless internet access, and visitor network connections. This is the highest risk zone because anybody can connect to it anonymously.
- **Non Card Data Business Environment –** Systems not used for payment processing, but are still business owned fit into this segment. These are systems that can be used for email, web browsing, and other higher risk activity that you would never want to perform on your payment processing systems. On occasion, these systems will almost certainly become infected with malware and viruses. Once a computer in this zone is infected, the hacker or infection will spread to other `systems if they're not protected by a firewall. Note that if any systems in this zone handle credit card data, that data is being put at risk. This is a medium risk zone due to risk of occasional infection. By segmenting these systems into their own zone, the breach is contained. The hacker, malware, or virus doesn't reach your firewall protected payment processing zone.
- **Card Data Business Environment –** Systems used for payment processing fit into this segment. These systems should only be used for POS activity and should NEVER be used for any other reason. Should these computers become infected with malware or viruses, sophisticated hacking tools can potentially steal sensitive data such as credit cards. This is a low risk zone because it's protected from the other two zones and high-risk activities such as web browsing and email do not occur inside it. The chance that hackers, malware, or viruses spread to these systems is minimal.

In summary, to segment your network for security you should:

- Protect both business environments from the untrusted environment
- Protect your card data business environment from the non-card business environment

Best Practices for Dedicated Networks

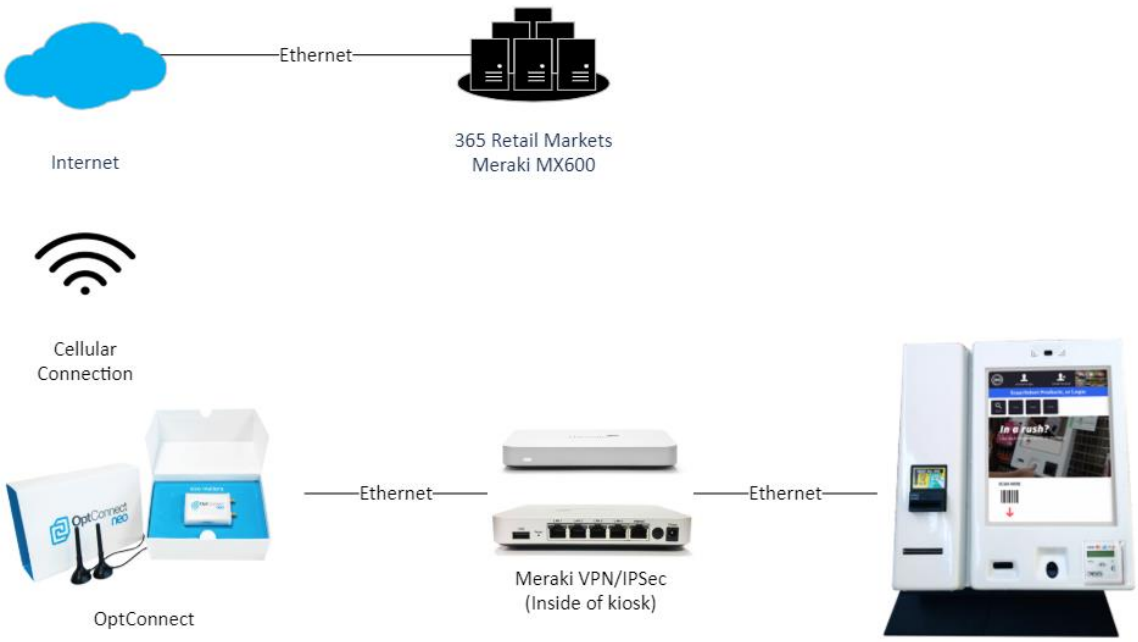
- Always change vendor supplied passwords on DSL or cellular modems. Do not leave default passwords on any of your network devices.
- Keep your network devices (modems, switches, routers) in a secure, locked area
- Disable all Wi-Fi broadcasts from modems

V5 Security Guide for Clients

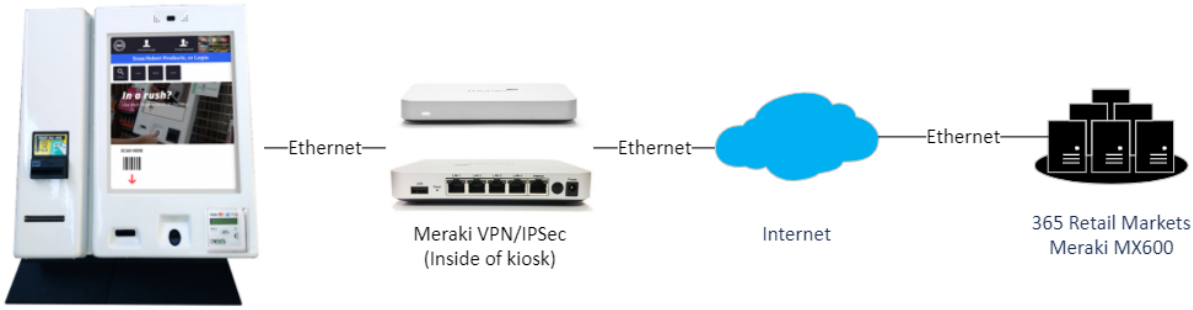
- Upgrade the firmware on your devices regularly. Manufactures often deploy security patches to their devices. You are responsible to ensure your device firmware stays up to date.
- A dedicated network is your Card Data Business Environment. Do not use it for any purposes other than those critical to your business. This includes only the services outlined in the Kiosk Technical Network Requirements document.

V5 Security Guide for Clients

V5 Kiosk with Cellular



V5 Kiosk with Ethernet



09/04/2019